

ORIGINAL

EDOK - Search Warrant (Revised 5/13)

United States District Court

EASTERN DISTRICT OF OKLAHOMA

In the matter of the search of 0:

Case No. 23-MJ-309-DES

Samsung Galaxy A14 smartphone, IMEI#
352678733599119 and an Acer Computer Model#
N20C5, Serial# NXAASAA001128052503400

SEARCH AND SEIZURE WARRANT

TO: ANY AUTHORIZED LAW ENFORCEMENT OFFICER

An application by a federal law enforcement office or an attorney for the government request the search of the following person or property located in the EASTERN District of OKLAHOMA (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT "A"

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

SEE ATTACHMENT "B"

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

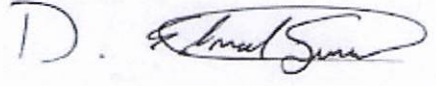
YOU ARE HEREBY COMMANDED to execute this warrant on or before December 21, 2023
(not to exceed 14 days)

- ☐ in the daytime 6:00 a.m. to 10:00 p.m.
☒ at anytime in the day or night as I find reasonable cause has been established

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Snow.

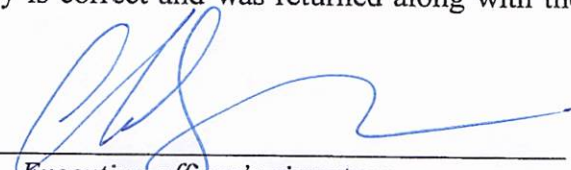
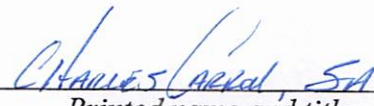
- ☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer after executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check):
☐ for _____ days (not to exceed 30).
☐ until, the facts justifying, the later specific date of _____

Date and time issued: 12/7/2023City and state: Muskogee, Oklahoma

Judge's signature

D. EDWARD SNOW
UNITED STATES MAGISTRATE JUDGE
Printed name and title



EDOK - Search Warrant PAGE 2

RETURN		
Case No.: 3056-OL-3848454 23-MJ-309-DES	Date and time warrant executed: 12-7-2023	Copy of warrant and inventory left with: N/A
Inventory made in the presence of: SA KAREN CASTIBLANCO		
Inventory of the property taken and name of any person(s) seized: <p>DATA EXTRACTION OF SAMSUNG GALAXY SMART PHONE IMEI 352678733599119</p> <p>DATA EXTRACTION OF ACER COMPUTER WEN2005 SERIAL# NXAASAA00128052503400</p>		
CERTIFICATION		
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.		
Date: 12-19-23	 Executing officer's signature	
	 Printed name and title	

ATTACHMENT A

The property to be searched is a black faced, Samsung Galaxy A14 smartphone, IMEI# 352678733599119 and an Acer Computer Model# N20C5, Serial# NXAASAA001128052503400. The Devices are currently located at the FBI, Durant Resident Agency, 201 N. 3rd Street, Durant, Oklahoma.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. §§ 1801, 2251(a), and/or 2252(a)(4) and involve CLYDE PARK CREWS III including:

- a. Photographs and/or video recordings depicting minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);
- b. Child pornography as defined by 18 U.S.C. § 2256(8);
- c. Photographs and/or video recordings capturing images of a private area of an individual without their consent and where the individual has a reasonable expectation of privacy;
- d. Data relating to the origin, ownership, and/or use of such materials; and/or
- e. Data relating to the user's intent to access, possess, or produce such materials, including search histories.

2. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors or a sexual interest in children, that were transmitted or received using computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

- a. Correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of

visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

- b. Any and all electronic and/or digital records and/or documents pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors;
- c. Any and all electronic and/or digital records and/or documents including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors;
- d. Any and all records of Internet usage including usernames and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums;
- e. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;
- f. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

3. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software;

4. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

5. Items or files containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized;

6. Correspondence, to include emails and chat logs, or other documents (whether digital or written) pertaining to the production, possession, receipt, origin, or distribution of images involving child pornography, children engaged in sexually explicit conduct, and/or video voyeurism; and

7. Any and all information, correspondence (including emails), records, documents and/or other materials related to contacts, in whatever form, with minors involving the production, possession and/or distribution of child pornography and the attempt or act of educating, enticing, coercing, or persuading a minor to engage in sexual acts.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and

instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.